2005 version
Ipv6 Deployment Guideline

SOHO segment

March 2005

IPv6 Promotion Council of Japan

DP-WG SOHO SWG

Table of contents

Introduction

This document is intended for system integrators who engage in SOHO configuration and users/administrators who are considering deployment of systems and is intended to describe general items, guidelines and methods that should be considered with regard to use of Ipv6 in SOHO environments.

Information described in this documents is not intended to be the sole solution but to show one example of a way of thinking. This document is created in such a manner that readers will be able to apply referring to this when they think about introducing Ipv6 according to their own guidelines.

SWG Members

Inquiries

For questions related to this guideline, please send E-mail to the following address:
Ipv6 Promotion Council of Japan DP-WG / e-mail: wg-dp-comment@v6pc.jp

1. Segment Features

SOHO Classification

Business offices called SOHO include the following:

・Family type operations

System configuration with one PC and Internet connection line. This type of environment is similar to the home segment environment.

・Small business offices (Independent SOHO)

Enterprise that carries out business activities based on a single small base. In addition to the configuration in item 1. above, the system is configured with more than one PC and a single subnet LAN.

・Small sales offices (dependent SOHO)

A small base of a larger sized organization. In addition to the configuration in item 2. above, the system is connected to an external network (Headquarters, ASP Center) via VPN.

・Convenience stores

The system includes POS terminals and Non-PC terminals. Many networks have a unique configuration.

In this deployment guideline, small business offices (hereinafter “Independent SOHO”) and small sales offices (hereinafter “dependent SOHO”) are the targets.

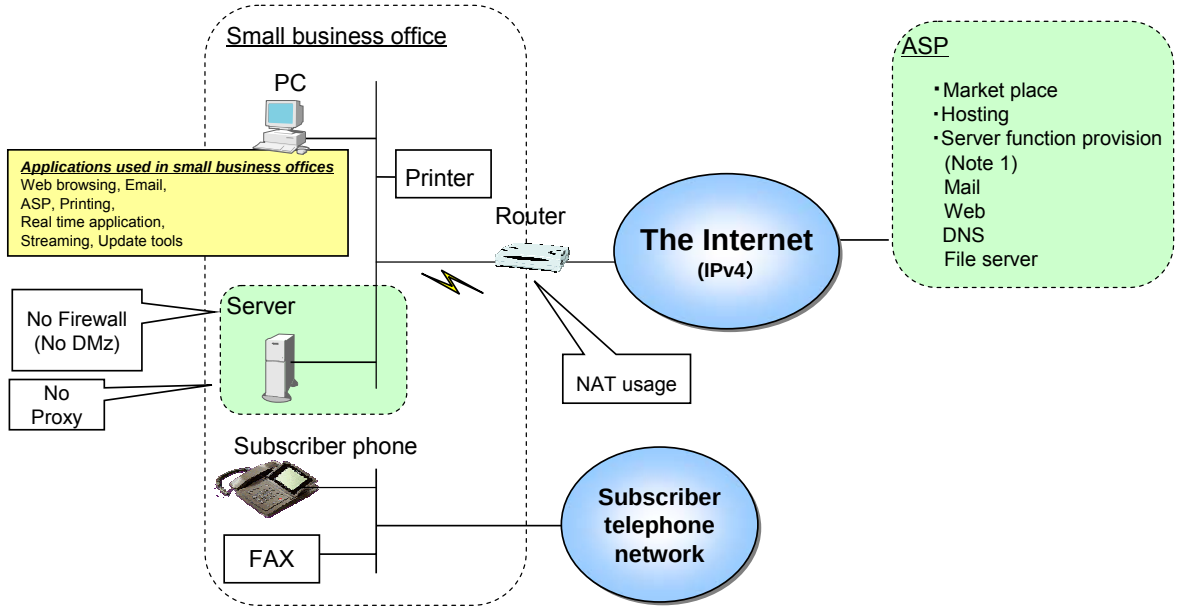
Present SOHO Network

Independent SOHO

Networks are used to exchange emails outside of the company and for Web browsing via the Internet. They are also used for ASP usage and sales web sites configured independently.

Concept of independent SOHO

Networks are used to exchange emails outside of the company and for Web browsing via the Internet. They are also used for ASP functions and to manage the sales websites the offices establish.

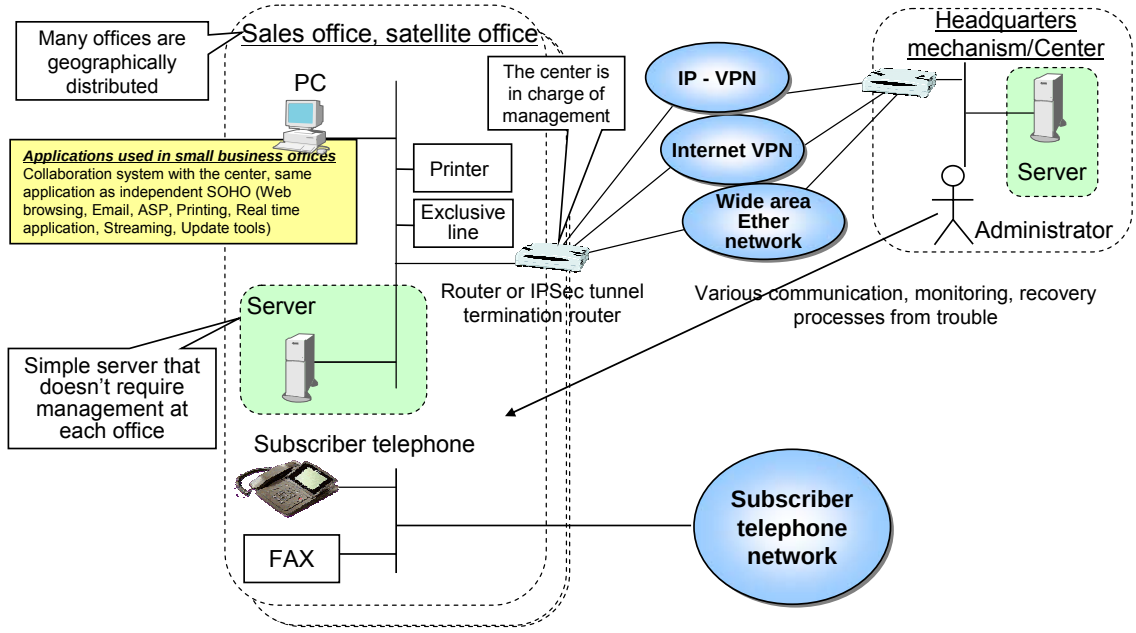


Dependent SOHO

The basic configuration is the same as that of independent SOHO, however, the system is connected to the center where administrator serves through IP-VPN, Internet VPN or wide-area Ethernet network.

Concept of dependent SOHO

The basic configuration is the same as that of independent SOHO, however, the system is connected to the center where administrator serves through IP-VPN, Internet VPN or wide-area Ethernet network.



2. Deployment Scenarios

Deployment steps

This section describes the deployment phases by dividing them into three steps: the currentIPv4 usage phase, initial Ipv6 deployment step (Ipv6 : Ipv4 = 1: 9) and full-scale Ipv6 deployment phase.

Two scenarios in the initial deployment step

In the initial deployment step of Ipv6, two scenarios can be anticipated depending on the purpose of deployment.

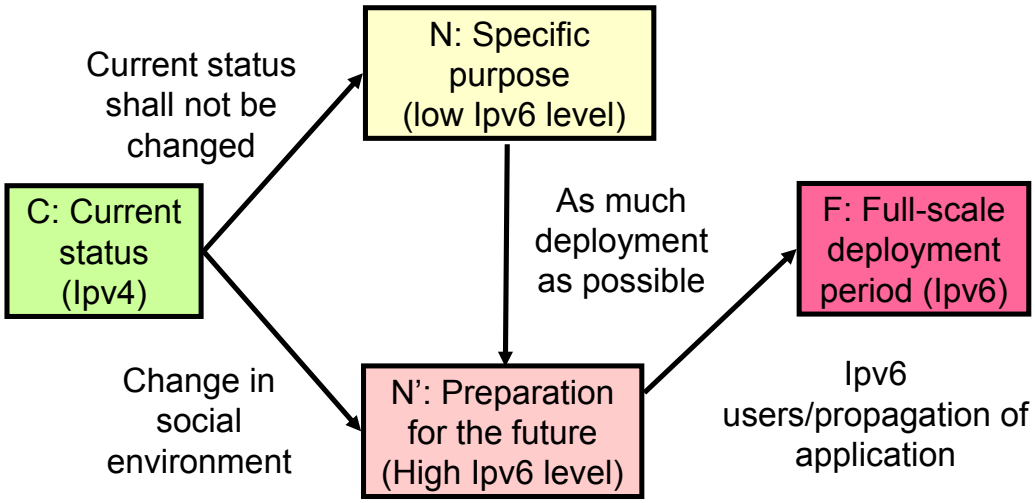
① Deployment for specific purpose
In this case, Ipv6 is deployed for some business purpose. This is triggered by certain factors, for example, when an application such as IP phone or instant messaging begins to use Ipv6, or when business partners migrate to Ipv6 to reinforce security for business transactions or maintenance purposes. This scenario basically does not change the Ipv4 network and can be considered to be a conservative Ipv6 deployment scenario.

② Deployment to prepare for the future
This scenario assumes that Ipv6 will be adopted in future and prepares for the use of Ipv6 when the system is replaced. This can be considered to be an active Ipv6 deployment.
In this guideline, it is assumed that the current Ipv4 usage changes in two ways, one is when Ipv6 is deployed for a specific purpose and the other is when Ipv6 is deployed in preparation for future activities. It is also assumed that Ipv6 deployment based on a specific purpose evolves into active Ipv6 deployment for the future and moves to a full-scale deployment phase in the end.

Relationship between scenarios

The illustration below shows the flow from the current situation (C) to the full-scale IPv6 deployment phase (F) including the two scenarios discussed above. Specific purpose (N) preparation for future (N') is assumed to be in one year and the full-scale deployment phase (F) is in two to four years.

Relationship between scenarios



Classification	C: Current	N: Next	N': Next'	F: Future
Time	Now	One year time	One year time	2~4 years time
Network content	Before migration	Simple Ipv6 migration	Full-scale Ipv6 migration	Complete Ipv6 migration
Ipv4/Ipv6 communication	Ipv4 only	Tunneling, Translator	Dual Stack	Ipv6 native/Dual Stack

① Network

・Classification of communication terminals

Terminals that communicate only inside LAN

Terminals that communicate both inside LAN and with the Internet

Terminals that communicate only with the Internet (e.g.: a telephone without an extension function)

・Type of links used

・IP address (distribution, setting, communication)

② Application

・Information-related communication: Web browsing, Email, ASP

・Real time communication: Printing, VoIP, Streaming

・Management-related applications: UpnP, Update tool

③ Security

・Network security

・Terminal security

3. Migration of Independent SOHO

Overview of Independent SOHO

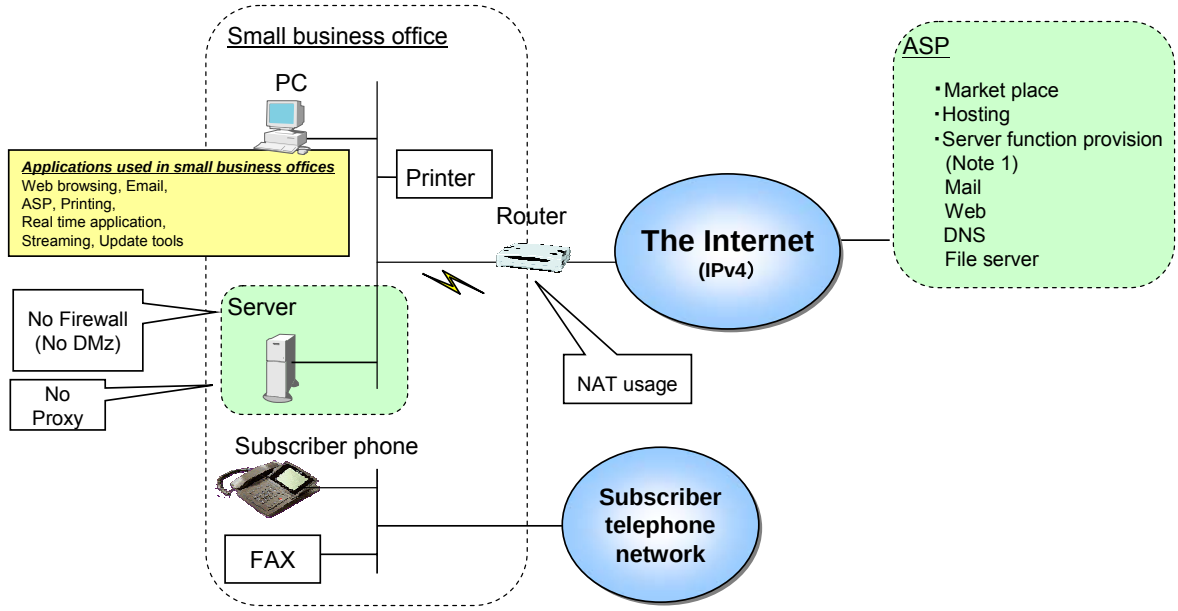
We consider small offices of independent businesses to be examples of independent SOHO operations. Typical examples are accountancy or design offices that have about 10 staff, and generally speaking the IT skill level is not particularly high. In some cases, there are some people who are familiar with IT.

The office is in one location and staff travel to various locations. Staff communicate with personnel in other companies, staff on business trips and employees' family members. Because their business is small scale, there is little budget for networking and they usually have no complicated servers.

Terminals used in independent SOHO operations are mostly PCs, and sometimes fileservers. They also have office equipment including printers, telephones and facsimile machines.

Image of independent SOHO

Networks are used to exchange Emails outside of the company and for Web browsing via the Internet. They are also used for ASP functions and to manage the sales websites the offices establish.



Migration of Network

(1) Network

① IP address to be used

Analysis

Because it is possible to grant a global address inside a LAN, it becomes possible to have communication with the global environment. Several patterns (/64 ~ / 48) are considered for global prefixes (dynamic/fixed) provided to LANs and prefixes provided inside a LAN. Because their business scale is small, the scope of addresses shall be less than /48.

Since at this stage a source address selection function is not implemented in applications, it is necessary to try various measures for communication using multiple prefixes.

In addition, in offices of this size, multiple segments make communication management such as printer connections or file sharing complicated. Therefore, generally a one segment configuration is used.

In the near term

For the above reasons, it seems that of the available global prefixes, /64 is generally used. Since the configuration is one segment for the time being, it does not seem that an additional prefix will be necessary.

Issues

We need to investigate how to handle addressing when a /64*n global prefix is used in the future.

② DNS related issues

Analysis

Implementation of DHCPv6 is limited to Linux, etc. at present, therefore it is not implemented on OSs such as Windows. However, it is possible to reference Ipv6 host information using the Ipv4 DNS. For some broadband routers, proxy DNS queries have already been implemented.

In the near term

Therefore, it seems reasonable to share the Ipv4 DNS and have the router perform DNS querying to handle Ipv6 name resolution under the present circumstances.

Issues

It is a task for the future to solve this problem (usage method of DHCPv6, etc.).

③ Link form

Analysis

For connection with ISP, two services are provided at present; tunnel connection and native connection.

In the near term

It is OK to select a tunnel connection when the existing environment is used as is, but this requires complicated router settings. Moreover, many tunnel connections do not support automatic setting of network addresses. On the other hand, the ADSL native connection service used in many SOHO environments supports auto address assignment. We recommend the native connection if simple settings are desired.

(2) Devices required for network migration

Devices required for network migration of independent SOHO are as follows.

Terminals

PCs and servers using an OS that supports IPv6

The latest versions of all the most commonly used OSs support Ipv6 (Windows XP, MacOS, Solaris, Linux, etc.).

Router

A broadband router that supports Ipv6

As a required function for Ipv6, Router Discovery is supported and also the DHCP Prefix Delegation mechanism may be used by some ISPs, thus it is necessary to implement this mechanism. Furthermore, when using the tunnel connection, an Ipv6 over Ipv4 tunnel function is

required.　Ipv4 function is also essential as well under present circumstances.

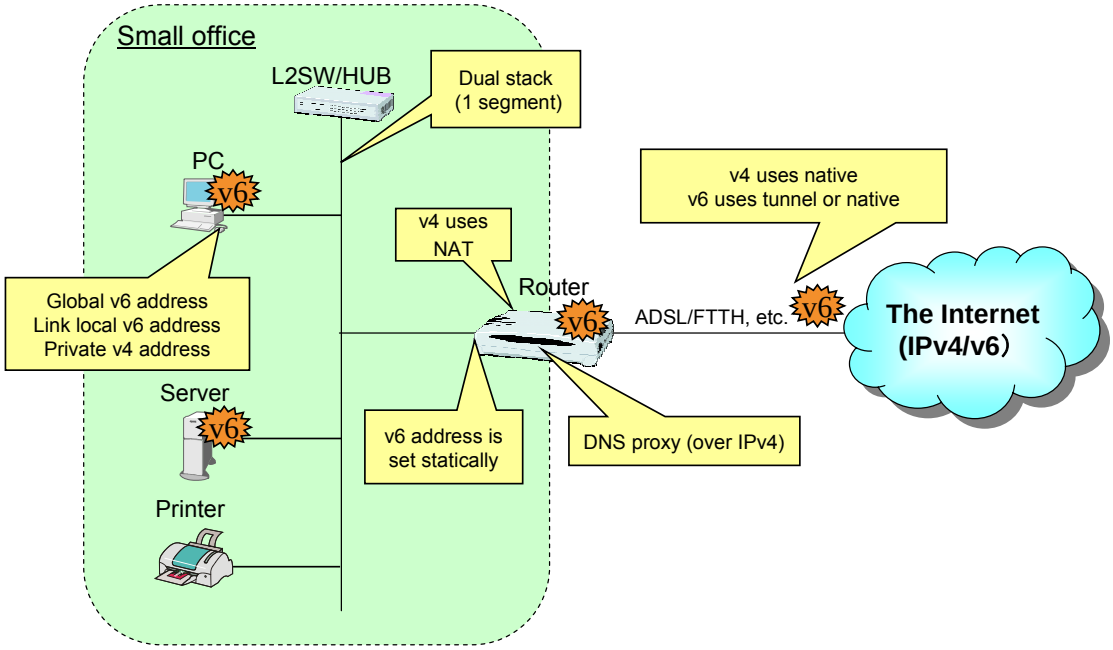
LAN switch/hub

If the layer 3 switch function is not used, currently available products are sufficient. However, even if only the layer 2 switch function is used, some switches check the type value and do not pass any type other than Ipv4.　It may be necessary to check the switch if it is old.

(3) Network image in near term / limited deployment case

In the near term, networks for specific purpose deployment (limited deployment) are as shown below.　For connection with an ISP, either a dual stack connection service with Ipv4 is used or tunneling of Ipv6 on the Ipv4 connection service is used.　Ipv6 network prefixes are set statically on the router.

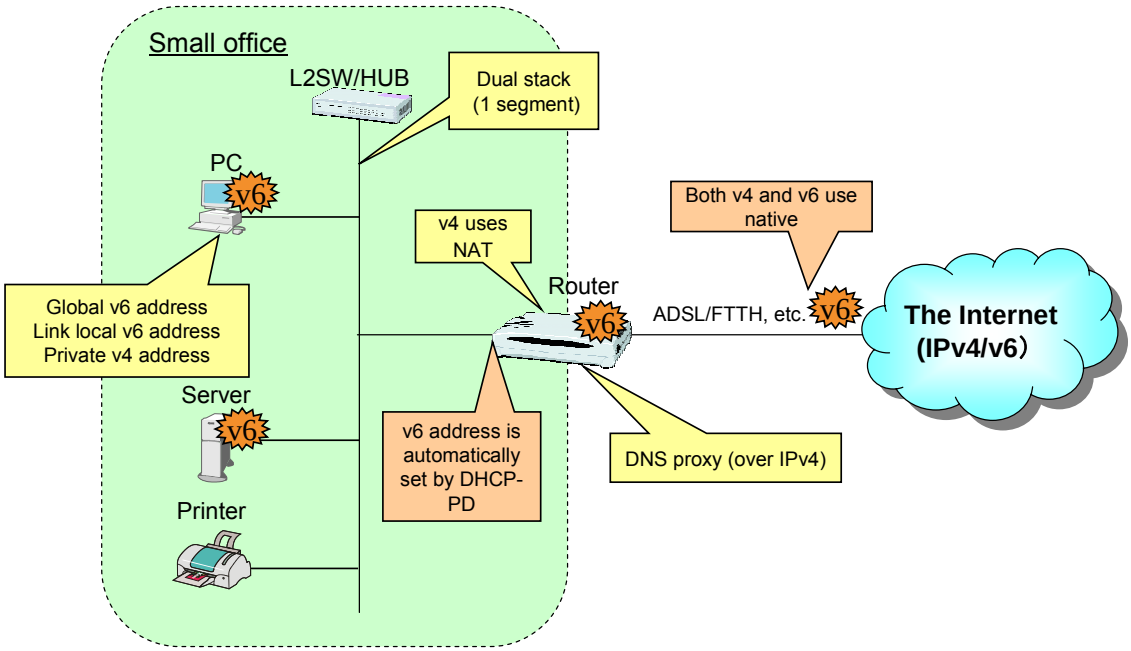
Network concept in near term / limited deployment case



(4) Network image in near term / active deployment case

In the active deployment case, an Ipv4/Ipv6 dual connection service is used as shown below. The Ipv6 network prefix is automatically set on the router using DHCP-PD.

Network concept in near term / active deployment case



(5) Summary of network migration

It seems OK for the time being for one /64 global prefix to be assigned for the IP address used by an independent SOHO. Depending on the application for which the network is used or if ISP service diversifies, use of multiple network prefixes may become effective.
For connection with an ISP, a tunnel or native connection may be selected depending on the need.
With regard to the DNS, Ipv6 address resolution is performed by Ipv4 transport for the time being. For this matter, it is efficient to use the Ipv4 DNS proxy function of broadband routers.

Migration of application

(1) Analysis of current state of applications

With an independent SOHO, the server for applications (mail, DNS, WWW, etc.) is usually configured on the LAN or provided by an external network. Sometimes an ASP or marketplace is used. As a mechanism to supplement communication between a private address and external

network, UpnP is used in some cases (communication tools, etc.).

PKI collaboration and RAS (Remote Access Service) are not used very much and generally certification is handled through server certification on a browser. However, in the future it is expected that client side certification collaboration using USB tokens, etc. will increase. With an independent SOHO, applications (file sharing, printing, etc.) operating on a closed LAN are used.

(2) Migration of applications

① Web browsing

Analysis

As a security issue, virus check software including Norton, Trend Micro does not supportIPv6. Also, privacy issues can be pointed out, such as recognition of originating IP address information by the Web server a user is communicating with.

Consistency with Ipv4 is ensured in a dual stack environment. If an Ipv6 single stack is used in future, a proxy or translator becomes necessary. Such devices are installed either at the ISP or within the site.

In the near term

A dual stack environment is required till anti-virus software that supports Ipv6 becomes available. Also it is hard to imagine that IPv6 only deployment at the Web server side will progress rapidly. As to security, it is safe to perform normal browsing with IPv4.

② Mail (between mail client and server)

Analysis

Very few mail client software applications currently support Ipv6. For that reason, virus checking software such as Norton and Trend Micro does not support Ipv6.

Usage form of client-server type Ipv6 mail is not different from Ipv4 mail. The difference from the Web is that the mailbox (accessed point) only exists at a location to which the user subscribes. On the other hand, the Web is used by connecting to many points.

The points that we must consider carefully when migrating from a dual stack environment to an Ipv6 only environment are the possibility of increased amount of SPAM and the risk that mail from specific addresses will not arrive. Furthermore, it is possible that association lists between IPv4 and IPv6 (such as the third-party relay lists) are used. There is also another possibility of the

usage of P2P mail, not client server.

In the near term

With regard to security, even when a mail client supports IPv6, if virus checking software does not support IPv6, it is necessary to prohibit IPv6. Mail is a client-server model that functions in the same way as Web browsing, therefore because there is less advantage in changing to IPv6, it is OK to use only IPv4 for the time being. Even though the change to IPv6 is put off for now, it may be appropriate to do so later observing the migration state to IPv6 by other applications.

③ ASP

Analysis

ASP services for SOHO environments include e-commerce, groupware and business-specific applications. Compared to large enterprises, in SOHO environments the need for front office related services such as information services is greater than back office-related services such as ERP.

From a protocol point of view, services can be classified into [Web-based ASP] and [proprietary protocol ASP] (communication tools other than the Web, such as Lotus Notes).

In the near term

For Web-based ASPs, it is adequate to handle Web based ASP in a same manner similar to Web browsing. For proprietary protocol ASPs, it may become possible to migrate to IPv6 automatically when a large number of software applications begin to provide IPv6 support.

④ Printing

Analysis

Sales of printers that directly connect to networks and support IPv6 have started recently. It is considered that printers that do not currently support IPv4 will support dual or IPv6-only in the future (in the case of client, IPv6 of Windows IPP is supported, etc.).

When a terminal (server) that supports IPv6 is connected to a printer, it becomes possible to print out using IPv6.

When IPv6 over IEEE1394, etc. goes mainstream, the connection protocol may possibly be IPv6-only. So, for a client of IPv4-only, PCs connected to a printer with IEEE1394 become printer servers, so that it would be appropriate if a function to process IPv4 querying were

furnished.
Furthermore, there is a possibility that IPv6 will be widely used in order to check the health of a printer and monitor the consumption status of consumable items remotely. However, there is a problem of security hole by auto communication between printer and server. There is already a hole checking service using telephone line of facsimile, so it is considered that this kind of service will be developed in the future.

In the near term

In the near term, IPv6 migration policy is such that local printing is possible even when a printer doesn't support IPv6. However, to satisfy the needs for remote printing, it would be convenient if IPv6 were supported. As printers support IPv6 more and more, it will be a trigger to migrate printing to IPv6.
In the present state, some printers go down if there is an IPv6 stream.

⑤ P2P application (excluding VoIP)

Analysis

Support for IPv6 during P2P communication is possible if the application supports IPv6. Since P2P communication is easily affected by NAT and there may be a reluctance to adopt flexible communication, IPv6 may hold certain advantages in this area. For instance, as opposed to IPv4 implementations, IPv6 IP phones do not need SIP-NAT, thus it is easier to deploy IPv6. In the case that a party on the other side of communication belongs to a specific group, IPv6 may be more convenient.
However, it is necessary to investigate security for direct communication. For example, it is required to prepare for the risk of a decrease in security for leakage of IP address information. Moreover, it is necessary to furnish a function to permit receiving communication only from registered terminals (high function such as changing/updating address is required).
On the network side, it is necessary to check the credit of a translator that goes through communication packet.
There is an advantage for Voice Chat that users are able to communicate directly to use a server (accounting collaboration). This advantage includes, for instance, specification of communication destination of existing network using phonebook function or assurance of scalability for presence management.

In the near term

In the near term, with regard to migration of P2P communication, if the application supports IPv6 and also the other party supports IPv6, it seems OK to actively use it. Also, it is possible to think about deployment of serverless type P2P communication.

⑥ VoIP

Analysis

・Limitation by NAT

In the case of IPv4, it is common to use NAT, therefore there is no problem for Gateway to terminate VoIP. However, in cases such as hard IP phones, it is not possible to have E2E communication when terminating telephone within LAN, therefore it is considered that a problem may occur on receiving of VoIP. It is possible to handle this problem if special NAT function is added to Gateway, but this may cause difficulty with regard to the cost of the Gateway. Therefore, IPv6 has more advantages because it is possible to realize E2E communication easily when VoIP is used in SOHO environments.

・Conversation between IPv6 and IPv4

For conversations between IPv6 and IPv4, NAT is required. Therefore, failure may occur when using in an existing general public network.

・Peer to peer phone

With regard to SIP, SIP servers are basically essential with IPv4. On the other hand, with IPv6, there are some models that do not use SIP servers. To ensure connectivity to an unspecified number, a phonebook function (DB function such as LDA) is required. However, if a VoIP Gateway has this function, communication with a specified number of parties is possible (SIP servers are not required in particular). For voice communication among over 3 parties, a SIP server model has difficulty but is suitable for direct communication between terminals. However, even with IPv6, it is possible to use a SIP server aiming at reduction of usage cost of terminals (function reduction).

・Necessary to investigate about security for direct communication

IPv6 has a risk of decrease in security caused by leakage of IP address information. Therefore, it becomes necessary to furnish a function to permit receipt of communication only from the registered terminals (high functions such as changing/updating addresses are required).

In the near term

When VoIP solution (hard phone in particular) that supports IPv6 is used, usage of IPv6 is recommended. However, it has a problem in communication with IPv4, therefore, it would be better to use, for example IPv6 for extension lines and IPv4 for external lines.

⑦ Video streaming

Analysis

The use of video streaming in SOHO environments is not so popular with IPv4 because, for one thing, less content is being sent than received and in the near term, inbound usage is the primary focus. However, it is considered that streaming has a merit if it supports IPv6 from the viewpoint of simultaneous viewing or multicasting. With respect to migration to IPv6, Windows Media Player already supports IPv6.

In the near term

There is no technical problem for migration. If attractive IPv6 broadcasting stations are available, support for IPv6 is worth investigating.

⑧ Update tool

Analysis

There are two methods of performing updates from the management center; Pull type updating and Push type updating. When IPv6 is supported, secure control of individual terminals is possible and Push type updates are easier to perform.

Primary functions include a control terminal search, multicasting and non-PC control. The client-server model is used for update tools for independent SOHO environments.

In the near term

For general update services (Windows Update, virus pattern file updates, etc.), it seems that IPv4 will only continue to be provided for the time being.

(3) Clients needing to migrate applications

Typical clients that can be used with IPv6 are as follows.

- ・Web browser: Microsoft IE、Firefox, OPERA, etc.
- ・Mail software: Win Biff, Edmax, Thunderbird
- ・Video streaming: Windows Media Player 9, 10
- ・IP phones: Some software phone applications support IPv6. Hard phones produced by Iwatsu Electric Co., Ltd.

As applications that become more advantageous when they support IPv6, there are real time (P2P) and streaming applications. With IPv6, one significant advantage is that NAT is not required.

A point of some concern is that, for reasons related to use of the Web and the DNS system, the current IPv4 network is also required. We believe applications that support IPv6 should be selected according to purpose. It is also necessary to confirm whether servers or subscribed services support IPv6.

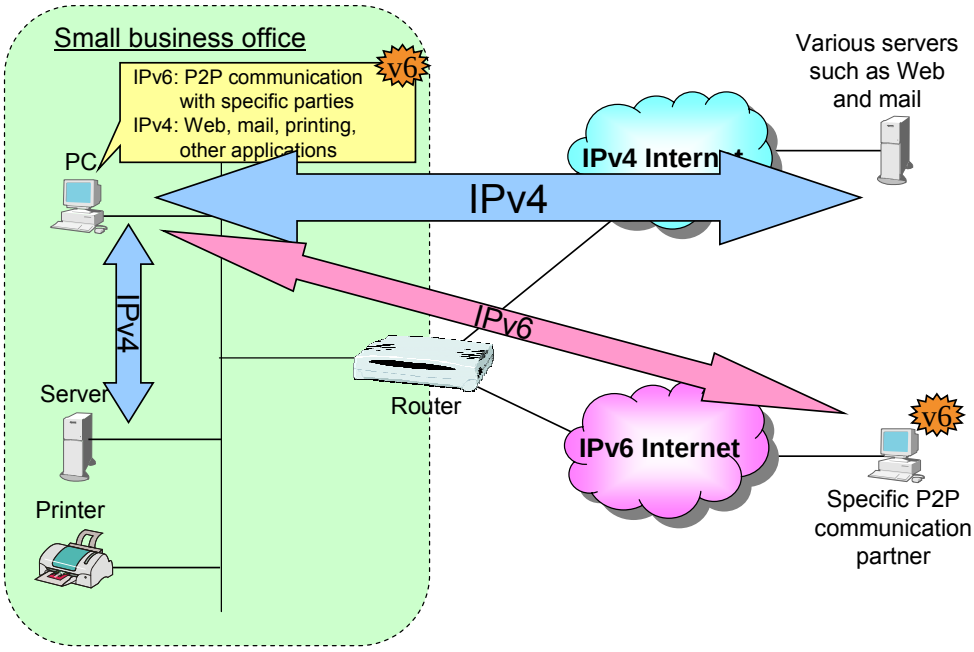
(4) Summary of applications

It is worth changing P2P communication with specific parties to IPv6. Since NAT is not required, the cost for address or port management can be reduced and it is advantageous for performance (delay, throughput) as well. There are fewer advantages for migrating current IPv4 applications such as Web browsing and email to IPv6, and the risk is rather high when changing to IPv6 in terms of security.

(5) Application concept in near term / limited deployment case

In a limited deployment scenario, IPv4 is used for Web applications, email and printing, and IPv6 is only used for P2P communication with specific parties.

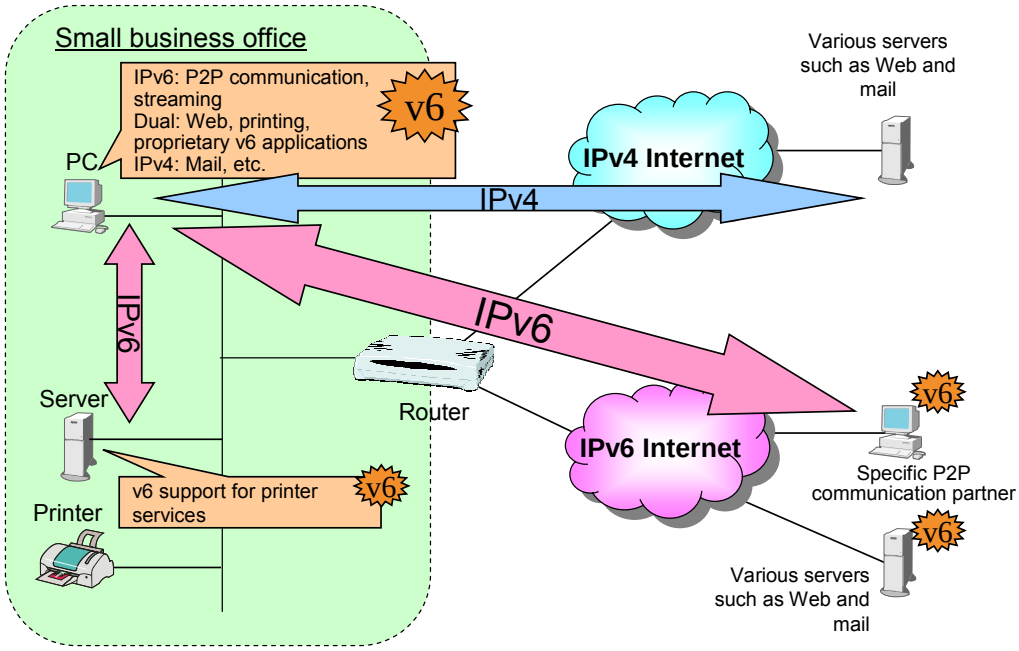
Application concept in the near term / limited deployment case



(6) Application concept in the near term / limited deployment case

In an active deployment scenario, P2P communication and streaming are migrated to IPv6, while Web and printing use the dual protocol and proprietary applications use IPv6 as well. Email continues to use IPv4.

Application concept in the near term / active deployment case



Migration of Security Management

* Details of security are included in the SWG material, so please refer to it.

① Gateway security

Analysis

● Encryption

Encryption for communication is necessary for telephone/fax, remote access by employees, business outsourcing and remote maintenance. Direct IPsec communication is performed between terminals, and devices such as sensors perform IPsec communication via a gateway. In this case, it is required to standardize devices in the communication path so that encrypted communication is not disturbed.

● Measures to prevent unauthorized access

When implementing E2E communication with IPv6, unlike UPnP, IPv6 does not require a mechanism to open a port by itself. Therefore, there is no need to be concerned about security holes that are related to the port opening mechanism. However, when terminals in an office are registered in an open DNS, they may be subject to certain types of attack.

Therefore, protection by filtering becomes necessary. Stateful packet inspection is performed and traffic is controlled on a terminal or port basis. Windows XP includes a personal firewall that supports IPv6, so usage of this can be considered as an option.

● Virus measures

Simple IDS is used. In this case, it is desirable that attack pattern files are retained in the firmware and both firmware and attack pattern files can be updated automatically. Until provision of virus checking products that support IPv6 begins, we recommend that the use of mail with IPv6 be prohibited.

● DoS attack measures

With IPv6, accessibility loss from outside by NAT can be improved, but each terminal may receive a DoS attack. As a countermeasure for this, IDS needs to support IPv6.

● Firewall

With regard to firewalls, as with IPv4, stateful packet inspection is used.

● Difference from IPv4

With regard to Gateway security, even if IPv6 is deployed, the model is the same as with IPv4 apart from P2P for the time being.

In the near term

The model the same as with IPv4 is used for the time being, such as usage of stateful packet inspection. When performing P2P communication, it seems better to limit communication in which the address of the parties can be specified and open the port.

Issues

One issue is the difficulty in configuring security policy settings for P2P communication-related use. It is desirable for a means to be provided by which users without expert knowledge are able to correctly set addresses of communication destinations, etc.

② Terminal security

Analysis

To safely perform P2P communication, it is expected that IPsec communication termination at terminals will be enabled. However, when open DNS registration is used, if the host address of terminals is disclosed, there is a risk that the level of security will fall.

With regard to terminal security related matters, the elements of IPv6 that have not progressed sufficiently include packet filtering (personal firewall, etc.) for hosts, IDS and virus checking. In addition, with regard to virus measures, IPv6 support is expected with respect to function updating via pattern Push from centers. Regarding the Windows standard PKI function, IPv6 support in ESP (encryption, etc.) is required.

On the other hand, functions that can be used as is on the IPv6 network include checking at application level (file infection checking, etc.), use of Ids/passwords, server certification retention by browsers and use of PKI or IPsec by dedicated clients.

In the near term

It is possible to use a model similar to IPv4. Use of only Ids/passwords and use of Web server certification have no problem. For P2P communication, at the moment it seems common to handle with gateway, but in the case of some products, it is possible to ensure security at the terminal level.

Issues

It is desirable for virus checkers and personal firewall products to provide IPv6 support. It is also expected that there will be common ideas about how to ensure security at the terminal level. For this, it is required that the setting of tools become simpler.

③ Summary of security

With regard to IPv6 migration in independent SOHO environments, the following security issues can be addressed.

For encryption, first of all, the IPsec tunnel mode function built into some routers and encryption using dedicated clients are used. SSL level encryption is valid with IPv6 as well.

With regard to measures to prevent unauthorized access/DoS attacks, stateful packet inspection is used for normal client-server type communication and filter-based security is used for P2P communication. Filter-based security is effective when the communication partner (address) is fixed. To the greatest extent possible, terminal addresses on a network should not be registered

in the open DNS.

With regard to terminal security, application level tools (virus checking of files, etc.) are valid with IPv6 and can be used continuously. Some personal security tools (mail virus checking tool, etc.) do not operate with IPv6, thus it is better if applications do not support IPv6 if there is no reason to do so. In addition to terminals, because it is easy to configure security settings that collaborate with a gateway, we recommend that both terminal and gateway filters be used.

④ Security concepts in the near term / limited deployment case

In the limited deployment scenario, encrypted communication with specific parties is performed using IPsec between gateways via the IPsec function of routers, etc. If encryption is desired for IPv6 communication, encryption on IPv4 shall be performed. When communication with other parties is needed, holes are punched in the router for that purpose. Boundary security related to IPv6 shall be handled through filtering.

Security concept in the near term / limited deployment case

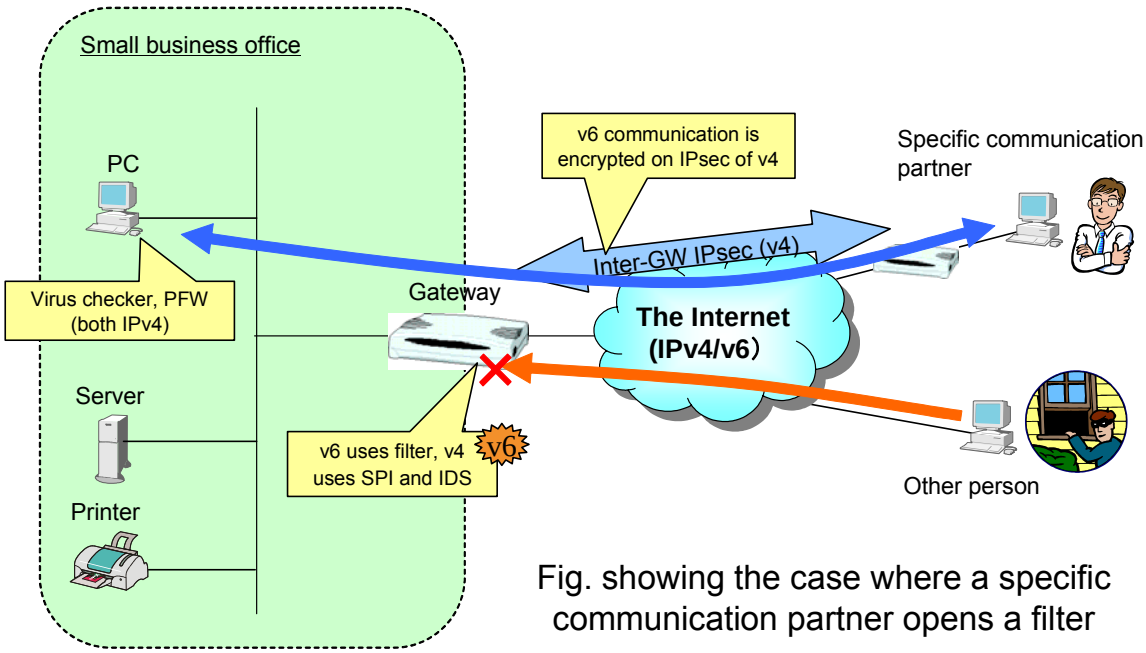
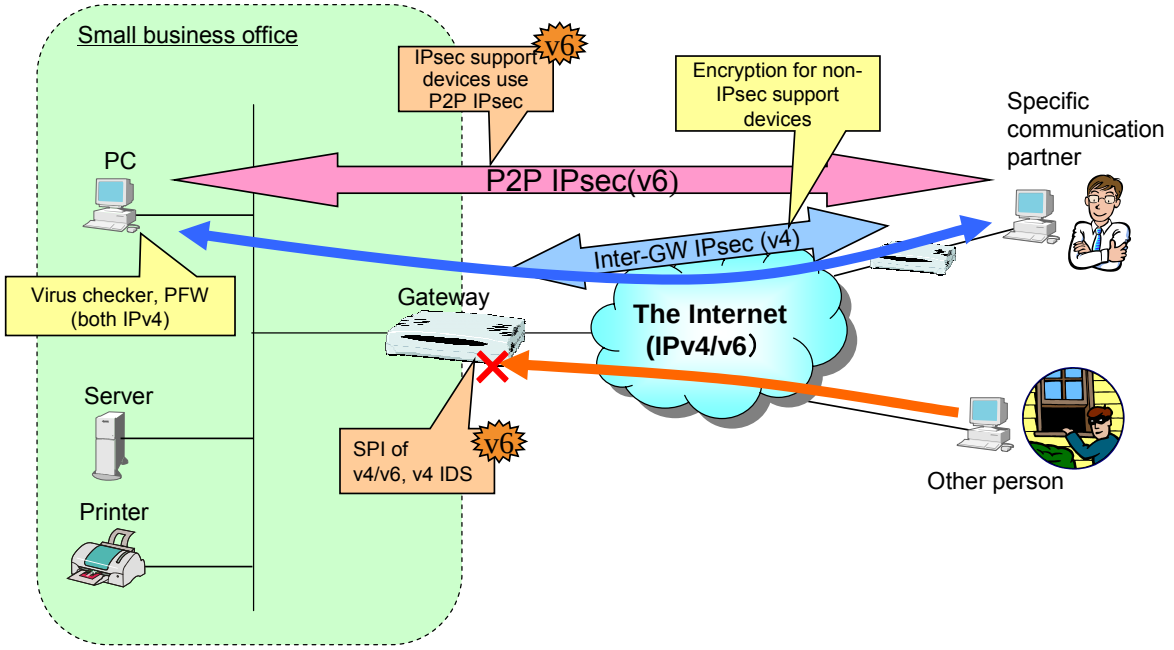


Fig. showing the case where a specific communication partner opens a filter

(5) Security concept in the near term / active deployment case

In the active deployment scenario, communication with specific parties can be protected using IPsec between gateways and peer-to-peer encryption is used for IPv6 devices that support IPsec. For communication with other parties, a stateful packet inspection firewall that supports IPv6 is used.

Security concept in the near term / active deployment case



Summary of migration in independent SOHO environments

For migration of IPv6 in independent SOHO environments, migration of network, application and security can be summarized as shown below.

Summary of network migration

Item	C: Current	N: Next	N': Next'	F: Future	Issues
Link used	PPP, etc.	Tunnel from router or terminal	Dual Stack	Native	
LAN address	Private address	Dual Stack, Single /64	Dual Stack, Single /64	IPv6 only, Multiple /64	Management when multiple prefixes are used
IP address distribution from ISP to user	PPP, etc.	Static	Auto allocation (DHCP PD is used)	Auto allocation (DHCP PD is used)	
IP address distribution to LAN communication terminal	DHCP	RS/RA	RS/RA	RS/RA or DHCP(?)	
Setting of DNS to LAN communication terminal	DHCP	IPv4 is used (DNS query proxy)		IPv6 support in DHCP or RA Extension, etc.	Standardization

Summary of network migration

Item	C: Current	N: Next	N': Next'	F: Future	Issues
Link used	PPP, etc.	Tunnel from router or terminal	Dual Stack	Native	
LAN address	Private address	Dual Stack, Single /64	Dual Stack, Single /64	IPv6 only, Multiple /64	Management when multiple prefixes are used
IP address distribution from ISP to user	PPP, etc.	Static	Auto allocation (DHCP PD is used)	Auto allocation (DHCP PD is used)	
IP address distribution to LAN communication terminal	DHCP	RS/RA	RS/RA	RS/RA or DHCP(?)	
Setting of DNS to LAN communication terminal	DHCP	IPv4 is used (DNS query proxy)		IPv6 support in DHCP or RA Extension, etc.	Standardization

Summary of application migration

Item	C: Current	N: Next	N': Next'	F: Future	Issues
Web browsing (including Web base of ASP)	IPv4 access	IPv4 access, special server moves to IPv6	Dual Stack, Access	IPv6 access + Translator	Security checking tool
Mail	IPv4 access	IPv4 access	IPv4 access (client server), IPv6 access (P2P)	IPv6 access (client server, P2P)	Security checking tool (virus in particular)
Proprietary application	IPv4 access	IPv4 access(*)	Dual Stack access? (*)	IPv6 access? (*)	※：Depending on the manufacturer
Printing (including file sharing, etc.)	IPv4 access	IPv4 access	Dual Stack access (move printer server to IPv6)	IPv6 access	Make printer support IPv6
P2P (public)	IPv4 access (via SIP server + NAT)	IPv4 access (via SIP server + NAT)	IPv6 access (via SIP server and P2P)	IPv6 access (via SIP server and P2P)	Framework for P2P use
P2P (specific)		IPv6	IPv6	IPv6	
Streaming	IPv4 access	IPv4 access	IPv6 access (including multicasting)	IPv6 access (including multicasting)	
Update tool	IPv4 access (Pull type)	IPv4 access (Pull type)	IPv4 access (Pull type)	IPv6 access (Pull + Push type)	Security checking tool, Control terminal search

Summary of security migration

Item	C: Current	N: Next	N': Next'	F: Future	Issues
Encryption	IPsec is used by Gateway	IPsec is used by Gateway	IPsec or P2P IPsec is used by Gateway depending on the terminal	IPsec or P2P IPsec is used by Gateway depending on the terminal	Standardization of methods
Virus measures	IPv4 IDS	IPv4 IDS (IPv6 mail is prohibited)	IPv4 IDS (IPv6 mail is prohibited)	IPv6 IDS	Delay in IPv6 support by virus checkers
DoS attack measures	IPv4 SPI	IPv4 SPI	Dual Stack SPI	IPv6 IDS	Collaboration of name resolution and resource block escape function
GW Firewall	IPv4 SPI	IPv4 SPI + IPv6 Filter	Dual Stack SPI	IPv6 bidirectional SPI	Implementation + Incoming control
Terminal unauthorized access protection	IPv4 Personal-FW (PFW)	IPv4 PFW ※IPv6はGWで	IPv4 PFW ※ GW for IPv6	Dual Stack PFW	Implementation
Terminal access	ID/PW	ID/PW	ID/PW PKI(?)	ID/PW PKI(?)	Complicated settings

4. Migration of Dependent SOHO Environment

Overview of Dependent SOHO Environment

(1) Assumptions about dependent SOHO environment

Dependent SOHO environments mean the sales offices and local company offices. Insurance and travel agencies are also included, however, those businesses are basically direct offices. This type of office typically employs up to 10 staff and system administrators are situated at the centers, not at the actual offices. IT skills at these offices are not high.

These offices are found in scattered locations nationwide and staff primarily work in local areas. However, these offices need to have communication using a system or dialogical communication with headquarters. Since there are many offices, the company cannot spend a lot of money for each. In general there are no complicated servers in each office.

(2) Current state analysis of dependent SOHO environment

The terminals used are mainly PCs and the office also has business equipment such as printers, file servers, special business terminals such as host terminals, telephone and facsimile machines. Applications used include email, Web browsing inside an Intranet or Internet and local communication such as printing and file sharing. With regard to host (center) collaboration, transaction and file exchange are performed. SNA, etc. have been used as communication protocols, but there is a tendency to migrate to Web-based use. Usage of telephones and facsimiles is gradually migrating to an IP telephone system.

A center-based start type network configuration is used. In this configuration, IP-VPN, wide-area Ethernet and Internet VPN (gateway IPsec base) are used. Smaller offices use ISDN or DA128 for connections but it seems that ADSL will become the most popular choice in future. These are used for backup or separated for voice/information related use and business related use.

The general address structure is such that there is one WAN side address and the LAN side configures /24 private addresses. Each office uses a NAT or fixed address on a VPN. With regard to private addressing, all offices use the same private addresses in some cases. Some require policy routing for the Internet, Intranet or specific applications.

Protocols used include IPv4, NetBEUI, IPP and file sharing protocols for local communication, and IPv4, SNA, http/SSL, POP3/SMTP, 3217, H.323/SIP, RTP and DLSW for remote communication.

Security is intensively controlled at the headquarters. Security is not usually handled by each sales office, or if it is, only partial control is exercised. Gateways are used to manage line connections. Basically, there is no inward communication from the Internet. Virus checking tools are already installed on terminals. In some cases, Internet communication goes through a

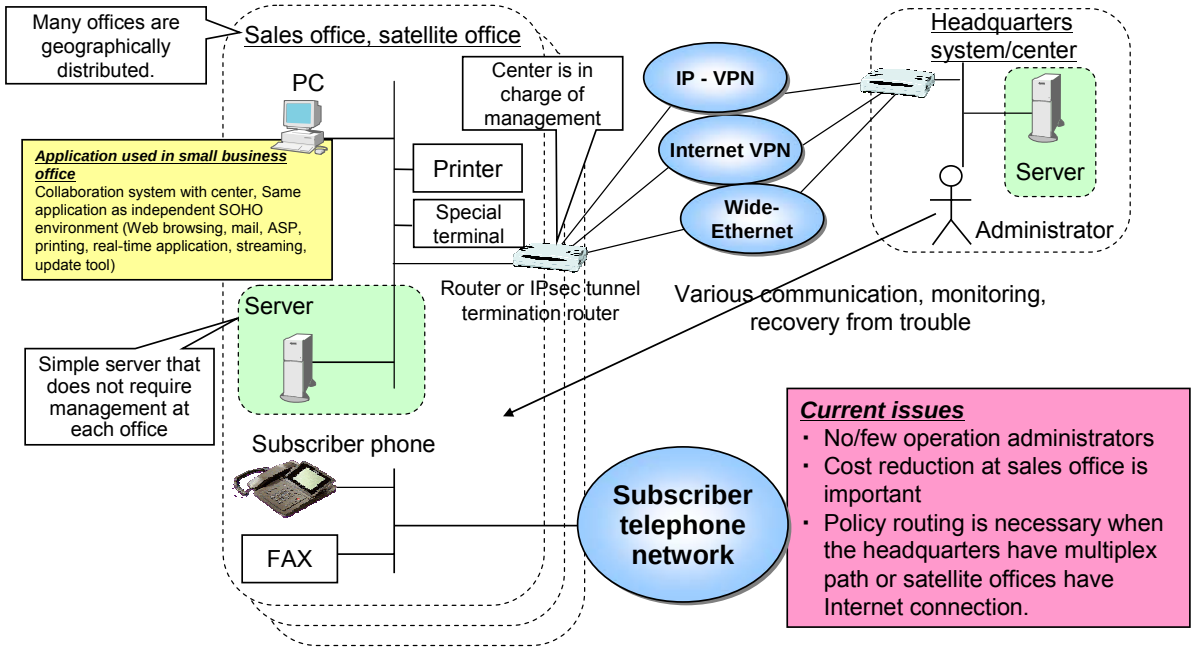
VPN and firewall at the headquarters.

(3) Concept of dependent SOHO

The dependent SOHO network configuration is similar to that of an independent SOHO environment, but is it is connected to headquarters system/center via IP-VPN, Internet VPN, wide-area Ethernet, etc.

Concept of dependent SOHO

Basic configuration is the same as that of an independent SOHO environment. It is connected to the center where an administrator is situated through IP-VPN, Internet VPN, wide-area Ethernet, etc.



Analysis of dependent SOHO environment migration

Migration of dependent SOHO environment is almost the same as that of an independent SOHO environment, with the difference being that the VPN must provide IPv6 support and the configuration of VPNs using IPv6 is desirable. Also, the needs of policy communication such as

QoS are considered. For details of routing with a multiple number of outward paths such as multi home, please refer to “Tips & Tricks”.
Unlike an independent SOHO, dependent SOHO uses legacy applications. Please refer to “Large Enterprise Guideline” for details of applications used.
Security is controlled by a gateway at the headquarters. Please refer to “Large Enterprise Guideline”. However, the router on the sales office side must be remotely controlled, and this issue is not covered in “Large Enterprise Guideline”.

Migration of VPN

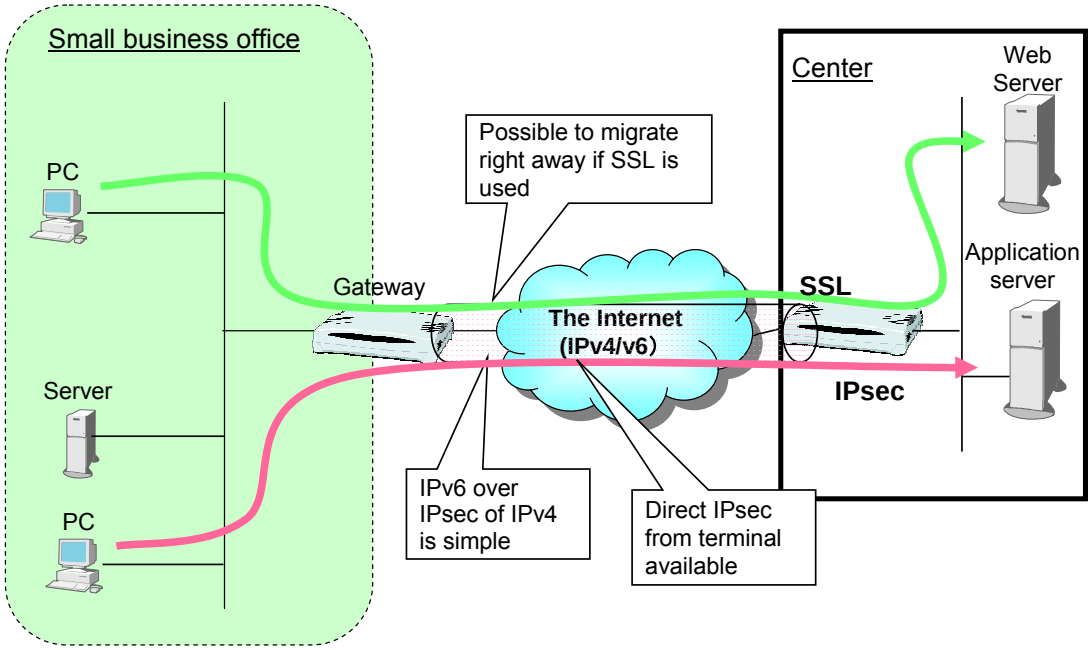
Analysis

VPNs can be executed as usual without the influence of IPv6 when using SSL server on the Internet. With IPv4, it is common to use a router-based tunnel in IPsec aggressive mode.
As options for the implementation of IPv6 in a VPN, there are IPv6 over IPv4 over IPsec, DTCP, IPv6 over IPsec IPv4 and IPsec IPv6 + Native service.
One problem with IPv6 over IPv4 over IPsec is that there are significant fragmentation effects. DTCP does not have an encryption function, thus it may result in fragmentation. IPv6 over IPsec IPv4 is a relatively low cost solution. IPsec IPv6 + Native service is excellent in terms of performance and extensibility.

In the near term

So, how should we deal with VPN for the time being? If it is SSL based, VPN can be used as usual by simply changing the stack to IPv6 and nothing else is required. IPv6 over IPsec IPv4 is suitable if VPN is lightly executed in the IP layer. If extensibility is emphasized, a native (including the dual stack) connection is appropriate.

Configuration concept of VPN



5. Future Usage Model

Concept of Future Usage

In future, various elements will be connected to networks by IPv6.
Since there is plenty of addressing and auto setting is sophisticated, a network interface allows easy use of not only PCs, printers, IP phones and PDAs, but also office equipment such as copying machines, FAXs, whiteboards, projectors and also peripheral PC devices, security cameras and time cards.
The spread of IPv6 may increase collaboration with external nodes. The reason for this is that streamlining of P2P communication and the security infrastructure provides a better environment for external collaboration. As a result, it is considered that the outsourcing of functions will increase.
Collaboration examples include the configuration of an order/reservation system (a Web-based system currently exists), inquiry/support desk function and telephone or videophone technology. Beside, IPv6 will promote collaboration with users outside of the company. Along with this development, the advent of IPv6-only nodes can be expected.
Mobile access will be commonplace, for example, a user may access the SOHO from outside the office to resolve names dynamically or exchange information via P2P, and information will be increasingly handled in real-time.

Issues of migration

As technical issues with regard to full-scale propagation of IPv6, naming, security, QoS, securing of reliability (multi homing) and translator (who provides the function) are considered.

6. Summary of Requests and Issues

Network

(1) Network

・The number of segments in a SOHO network

What size IPv6 address is provided to a user organization is left up to the ISP. Two types of IPv6 address are currently distributed by ISPs; the /64 prefix (for one segment) and the /48 prefix (for multiple segments).

One advantage of a single segment /64 prefix is that configuration is easy and auto assignment functions make it easy for users as well (of course, one segment /48 prefix assignment is possible).

The advantage of operation using a /48 prefix (/64 multi segments) is that policies can be applied to each segment flexibly. On the other hand, the complexity of policy management or operation management increases and management at a SOHO that does not have an administrator may become difficult.

・Prefix Delegation

In order to simplify settings in a SOHO environment in which there is no administrator, the auto setting function (called Prefix Delegation) for the network prefix from the ISP is required. Currently, the following Prefix Delegation methods are considered.

- MSR (Multi-link Subnet Router) model

This model handles the link between the CPE (Customer Premise Equipment：ADSL modem, etc.) and the PE (Provider Edge Device) and the LAN side link of the CPE as the same link. A single /64 prefix is assigned to the LAN side terminal. This exists in theory but for the time being is not supposed to be realized in actual service. This is because it is believed a large amount of ICMP router requests (Router Solicitation) would be sent to ISPs.

- Layer 3 router model

A layer 3 router that is a CPE terminates the network prefixes assigned from the ISP once and then distributes these assigned prefixes within the LAN side again. This model can target assignment of /48 or /64 prefixes. With regard to technology based on this model, DHCPv6-PD is major and approval as RFC has been completed.

・DNS Discovery

With IPv4, the minimum amount of necessary network information (IP address, default router, DNS server address) can be all obtained automatically by DHCP, and actually this method is generally used.

What about network information auto setting with IPv6? IPv6 provides a mechanism to obtain network prefixes or default router addresses by RA (Router Advertisement) from router. However, currently DNS server addresses are not distributed by RA. Therefore, the IETF is currently discussing the method to distribute DNS server addresses.

As candidate methods, the usage of well-known fixed addresses, extension of RA or extension of DHCPv6 (Stateless DHCPv6) are named.

(2) Notes related to applications

When the IPv6 single stack terminal/environment spreads, a translator or reverse proxy is required to access a IPv4-only web. These may be installed by an ISP, but implementation in a home gateway, etc. can also be used.

With regard to IPv6 migration of mail software, at this moment most existing security checking software does not support IPv6.

With regard to IPv6 support by ASP, it is possible that an ASP that uses proprietary protocol may need to modify applications.

When P2P application performs communication from v4 terminal to v6 terminal, the v4-v6 NAT device is required. However, due to the difference in address area sizes, it is difficult to map the v6 terminal in a fixed manner. Therefore it is necessary for the v4 terminal to negotiate with the NAT device somehow in order to acquire mapping information. For this purpose, the use of implementation by UpnP or DNS links is under consideration.

(3) Notes related to security

With regard to security, it can be pointed out that policy setting will be difficult as the communication style diversifies. It is required that there will be a means to correctly set communication destination address, etc. even though no person with expert knowledge is available.

Crucial infrastructure products such as virus checkers and personal firewall products need to support IPv6 as well. The popularity of security at the terminal level affects the degree of ease of configuration.

Other notes

MTU Discovery

With IPv4, fragmentation is possible even in the path of packet delivery, and ICMP such as ICMPv6 Type2 is not used. In some cases, ICMP packets are filtered at an ISP.
On the other hand, with IPv6, fragmentation in the path of packet delivery is not performed. When the packet size becomes too big at a router along the way, the router returns an ICMPv6 Type 2 “Packet Too Big Message” to the sender. The sender receives the message and repackages the packet into an appropriate size and sends it again. Therefore, on the Internet, if an ICMPv6 message (at least Type2) is not delivered to the end node, communication performance may be ruined, thus care must be exercised. It should be operated sufficiently with ISP so that ICMPv6 Type2 messages are not filtered out.

Host name registration

As the number of Non-PC devices (camera, printer, etc.) that can be connected directly to a network increases, the need to use them easily by connecting to a network will increase as well. In SOHO environments with no administrator, if it is possible, users would like to avoid registering IPv6 addresses (128 bit) manually each time for a PC. For that reason, it is required to provide a function to match the terminal name and address.
Auto registration method for the standard host name is still in the investigation phase. However, as available technologies, there are Dynamic DNS, UpnP (Universal Plug and Play) and SIP. For reverse search, a method called Node Information Query of ICMPv6 is available. Under this method, when a Node Information Query (Type 139 of ICMPv6) is sent to an address, a reply (Type 140 of ICMPv6) including Note Information (host name, etc.) is returned. The platforms currently compatible are UNIX’s FreeBSD, Linux, etc.

Application support

Currently, applications waiting for IPv6 support include DNS resolvers. The current situation is that the content of the resolver supports IPv6 but communication itself does not yet support IPv6.
With regard to security tools, application gateway type virus checking software (web, mail, etc.) still does not support IPv6. However, this is not a problem because the file I/O check type

software of an OS does not depend on IPv4/v6. It is also expected that update tools such as Windows Update and messenger applications such as Windows Messenger will be able to support IPv6.

(4) QoS

Along with the proliferation of broadband, the number of real-time applications is increasing, and we can imagine that when IPv6 spreads, P2P communication performance will improve and the needs for QoS will increase accordingly in the future.

With regard to QoS issues between PE-CPE, upstream QoS control is technically possible to some degree. However, due to cost issues, it is not actually implemented. In the case of downstream QoS control, it is basically difficult to do QoS from the end terminal side. But, the package shaping function of the broadband router can realize this to some level. These issues will probably lead to requests for services and functions on the ISP side or from device venders.

Deployment WG SOHO Segment Members

(titles are omitted)

SWG chairs

Inomata (Fujitsu Limited)
Sakauchi (NEC Corporation)
Tsukioka (Hitachi, Ltd.)

Members

Arano (Intech NetCore, Inc.)
Nakai (NTT Communications Corporation)
Nakahara (NEC Corporation)
Kanaumi (NEC Corporation)
Ohira (Ricoh Co., Ltd.)
Ito (Canon Inc.)
Yamamoto (Shimizu Corporation)
Yoshioka (Toyota Info Technology Center Co., Ltd.)
Ozaki (Fujitsu Limited)

Inquiries

For questions related to this Guideline, please send email to the following address:
IPv6 Promotion Council of Japan DP-WG / e-mail: wg-dp-comment@v6pc.jp